REMARKS

This communication is a full and timely response to the final Office Action dated January 26, 2004. By this communication, claim 1 has been amended to recite said processing control means accesses the generated private key, decrypts a symmetric key, and decrypts the encrypted text using the decrypted symmetric key when the user's next instruction specifies a decryption of an encrypted text; and said processing control means generates a symmetric key and a public key to encrypt the symmetric key when the user's next instruction specifies an encryption of plain text. In addition, claim 9 has been amended to recite the fingerprint identification apparatus accesses the generated private key, decrypts a symmetric key, and decrypts the encrypted text using the decrypted symmetric key when the instruction command specifies a decryption of an encrypted text, and the fingerprint identification apparatus generates a symmetric key and a public key to encrypt the symmetric key when the instruction command is one that specifies an encryption of plain text. Support for the amendment to claims 1 and 9 can be found variously throughout the specification and the claims. For example, support for the changes to each of claims 1 and 9 can be found at page 19 lines 1-18 and page 20 lines 4-24 of the specification. No new matter has been added.

In addition, claims 17-19 have been added. The subject matter recited in claims 17-19 was previously recited in original claims 6-8, which were canceled in a response filed on November 4, 2003. Reinstatement and reconsideration of this claimed subject matter is respectfully requested.

Entry of this Amendment is proper under 37 C.F.R. §1.116 since the amendment: (a) places the application in condition for allowance (for the reasons discussed herein); (b) does not raise any new issues requiring further search and/or consideration; (c) satisfies a requirement of form asserted in the previous Office Action; and (d) places the application in better form for appeal, should an appeal be necessary. The amendment is necessary and was not earlier presented because it is made in response to arguments raised in the final rejection. Entry of this amendment is respectfully requested. Reexamination and reconsideration in light of the above amendments and the following remarks is respectfully requested.

No new matter has been added. Claims 1, 2, 4, 5, 9-11 and 17-19 are pending where claims 1, 9, and 17 are independent.

Rejections Under §102

Claims 1, 2, 4, 5, and 9-11 were rejected under 35 U.S.C. §102(a) as anticipated by *Pare Jr. et al.*, U.S. Patent No. 5,838,812. Applicant respectfully traverses this rejection.

Independent claim 1 recites an authentication system used when stored information is manipulated, comprising a host computer comprising, input means for inputting a user's instruction; command output means for generating from the user's instruction an instruction command which requests a predetermined processing to be executed and for outputting the instruction command; and communication means for communicating with an external unit; and a fingerprint identification apparatus comprising, communication means for communicating with said host computer; processing control means for executing a predetermined processing according to the instruction command input from said host computer by said communication means; fingerprint detection means for detecting a fingerprint and for generating fingerprint data; storage-information recording means for recording the fingerprint data and storage information related to the fingerprint data; and fingerprint identification means for verifying fingerprint data detected by said fingerprint detection means with the fingerprint data recorded by said storage-information recording means, wherein said storage-information recording means stores a private key generated by the public-key encryption method, wherein said processing control means accesses the generated private key, decrypts a symmetric key, and decrypts the encrypted text using the decrypted symmetric key when the user's next instruction specifies a decryption of an encrypted text; wherein said processing control means generates a private key, symmetric key, and a public key to encrypt the symmetric key when the user's next instruction specifies an encryption of plain text; and wherein the user's next instruction is sent to the host computer through communication cable.

Similarly, claim 9 recites, among other things, said fingerprint identification apparatus accesses the generated private key, decrypts a symmetric key, and decrypts the encrypted text using the decrypted symmetric key when the instruction

command specifies a decryption of an encrypted text; and said fingerprint identification apparatus generates a symmetric key and a public key to encrypt the symmetric key when the instruction command specifies an encryption of plain text.

Pare Jr. discloses a system for identifying individuals for the purpose of performing financial transactions and non-financial transmissions, which can accommodate a large number of users. In particular, a data processing center 1 connects to various terminals 2 and computer networks 4 through a various types of communication mediums 3. A firewall machine 5 prevents electronic intrusion of the system and a gateway machine 6 executes the requests of the users, and decrypts data received from the various terminals. The various terminals can be any of a number of data entry and biometric devices 13. The terminal 2 communicates to other devices on the network via a conventional modem 18 using request packets 19 and response packets 20. During communication, certain portions of the request packets 19 and response packets 20 are encrypted while other portions of these packets are sealed. In particular, a when sending information to a data processing center 1, the biometric device 13 outputs an encrypted biometric–PIC block that includes a message key. That is each biometric-PIC block received by the data processing center 1 may also contain an optional response key. Before responding to a request that includes a response key, the DPC encrypts the reply packet with the response key. *Pare, Jr.*, however, fails to disclose, teach, or suggest at least accessing the generated private key, decrypting a symmetric key, and decrypting the encrypted text using the decrypted symmetric key when the user's next instruction is one that specifies a decryption of an encrypted text. Moreover, *Pare Jr.* fails to disclose, teach, or suggest at least generating the private key, the symmetric key, and the public key to encrypt the symmetric key when the user's next instruction is one that specifies an encryption of plain text. The Office Action argues that because *Pare Jr.* discloses that all communicated information is encrypted, any instruction command that the user submits would have to be an encryption of plain text. Applicant disagrees with this position and submits that *Pare Jr.* fails to disclose the functions performed by the processing means when performing a decryption or encryption operation.

To properly anticipate a claim, the document must disclose, explicitly or implicitly, each and every feature recited in the claim. *See* Verdegall Bros. v. Union Oil Co. of Calif., 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). For at least the reasons discussed above, Applicants respectfully request that the rejection of claims 1 and 9 under 35 U.S.C. §102 be withdrawn, and these claims be allowed.

Claims 2, 4, and 5 depend from claim 1, and claims 10 and 11 depend from claim 9. By virtue of this dependency, Applicants submit that claims 2, 4, 5, 10, and 11 are allowable for at least the same reasons given above with respect to their respective base claims. In addition, Applicants submit that claims 2, 4, 5, 10, and 11 are further distinguished over *Pare, Jr.* by the additional elements recited therein, and particularly with respect to each claimed combination. Applicants respectfully request, therefore, that the rejection of claims 2, 4, 5, 10, and 11 under 35 U.S.C. §102 be withdrawn, and these claims be allowed.

Newly Added Claims

Claim 17 recites a fingerprint identification apparatus in an authentication system used when stored information is manipulated, comprising communication means for communicating with a host computer; processing control means for executing a predetermined processing according to an instruction command input from the host computer by said communication means; fingerprint detection means for detecting a fingerprint and for generating fingerprint data; storage-information recording means for recording the fingerprint data and storage information related to the fingerprint data; and fingerprint identification means for verifying fingerprint data detected by said fingerprint detection means with the fingerprint data recorded by said storage-information recording means.

In contrast, *Pare Jr.* discloses a system for authorizing a transaction by correlating a user's biometric sample with an authenticated and stored biometric sample, where the correlation of the user's biometric sample with the stored biometric sample is conducted between two devices over a network. *Pare Jr.* fails to disclose, teach, or suggest a fingerprint apparatus that at least includes fingerprint detection means for detecting a fingerprint and for generating fingerprint data and fingerprint identification means for verifying fingerprint data detected by said

fingerprint detection means with the fingerprint data recorded by storage-information recording means. For at least this reason, Applicant respectfully requests that claim 17, and dependent claims 18 and 19 be allowed.

Conclusion

Based on at least the foregoing amendments and remarks, Applicants submit that claims 1, 2, 4, 5, 9-11, and 17-19 are allowable, and this application is in condition for allowance. Accordingly, Applicants request favorable reexamination and reconsideration of the application. In the event the Examiner has any comments or suggestions for placing the application in even better form, Applicants request that the Examiner contact the undersigned attorney at the number listed below.

Applicant believes no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 18-0013, under Order No. SON-1710 from which the undersigned is authorized to draw.

Dated: March 30, 2004

Respectfully submitted,

By _____
Ronald P. Kananen
Registration No.: 24,104
Attorney for Applicant

RADER, FISHMAN & GRAUER, PLLC
Lion Building
1233 20th Street, N.W., Suite 501
Washington, D.C. 20036
Tel: (202) 955-3750
Fax: (202) 955-3751
Customer No. 23353

DC146397

In the event additional fees are necessary in connection with the filing of this paper, or if a petition for extension of time is required for timely acceptance of same, the Commissioner is hereby authorized to charge Deposit Account No. 180013 for any such fees; and applicants hereby petition for any needed extension of time.